UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,351	06/29/2001	Joubert Berger	10013502-1	2270

7590 06/29/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
KENDALL, CHUCK O	

ART UNIT	PAPER NUMBER
2192	

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/896,351	BERGER ET AL.	
	Examiner	Art Unit	
	Chuck Kendall	2192	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/06/05 has been entered.

2. Claims 1 – 54 have been amended and are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1,10,11,13 –18 & 37, 40 – 47, & 51 – 54 are rejected under 35 U.S.C. 102(e) as being anticipated by Drake et al. USPN 6,347,374 B1.

Regarding claim 1, a system comprising:

operating system providing at least one routine capable of being invoked, and said operating system operable to collect raw audit data for invoked operating system routines (FIG.1, 26);

data storage having said raw audit data stored thereto and software code executable by at least one processor to receive said raw audit data (9: 45 – 60) and generate output comprising at least a portion of said raw audit data in a desired format defined by a template (FIG.1, 38, see destination directory and parameter, for format also see 2: 45 – 55, also see storage mechanism, also see 11:12 – 17 and 17: 25 – 40).

Regarding claim 10, the system of claim 1 wherein said template comprises at least one conditional element (2: 45 – 55, see compare, misuse engine and output mechanism).

Regarding claim 11, the system of claim 10 wherein said at least one conditional element dictates that said output is to have a particular format if a condition is satisfied otherwise said output is to have a different format (7: 25 - 31).

Regarding claim 13, the system of claim 1 wherein said operating system comprises a kernel-level audit device driver for collecting said audit data (9:55 – 60, see collector for different operating system for kernel level device driver).

Regarding claim 14, the product version of the system in claim 1, see rationale as previously discussed above.

Regarding claim 15, the computer program product of claim 14 wherein said raw audit data is collected by an operating system (9:55 – 60).

Regarding claim 16, the computer program product of claim 14 wherein said at least one routine includes at least one invoked operating system routine (9:55 – 60, see collector).

Regarding claim 17, the computer program product of claim 16 wherein said at least one invoked operating system routine is invoked by an application via system call (10:51 – 57).

Regarding claim 18, the computer program product of claim 16 wherein said at least one invoked operating system routine is invoked via user command (8:25 – 35).

Regarding claim 37, the software version of the system in claim 1, see rationale as previously discussed above.

Regarding claim 40, the system of claim 1 wherein said generated output comprises presentation output (17:55 – 58).

Regarding claim 41, the system of claim 40 wherein said presentation output presentation output comprises at least one selected from the group consisting of:

presentation output to a display, and presentation output a printer (17: 55 – 58).

Regarding claim 42, the system of claim 40 wherein said presentation output presentation output comprises at least one selected from the group consisting of:

presentation output by a browser, presentation output by a spreadsheet program, and presentation output by an application program (for at least one see, displaying and printing statistical data 17: 55 – 58).

Regarding claim 43, the system of claim 1 further comprising:

user interface for receiving from a user input defining said template (17:25 – 40).

Regarding claim 44, the computer program product of claim 14, wherein said code executable to generate output comprises:

code executable to generate presentation output (see, displaying and printing statistical data 17: 55 – 58).

Regarding claim 45, the computer program product of claim 44 wherein said presentation output presentation output comprises at least one selected from the group consisting of:

presentation output to a display, and presentation output a printer (17: 55 – 58).

Regarding claim 46, the computer program product of claim 44 wherein said presentation output presentation output comprises at least one selected from the group consisting of:

presentation output by a browser, presentation output by a spreadsheet program, and presentation output by an application program (for at least one see, displaying and printing statistical data 17: 55 – 58).

Regarding claim 47, the computer program product of claim 14, further comprising:

code executable to receive from a user input defining said audit transformation template (17: 25 – 40, & 55 – 58).

Regarding claim 51, which recites the library version of claim 44, see reasoning as previously discussed above.

Regarding claim 52, which recites the library version of claim 45, see reasoning as previously discussed above.

Regarding claim 53, which recites the library version of claim 46, see reasoning as previously discussed above.

Regarding claim 54, which recites the method version of claim 1, see reasoning as previously discussed above.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2 – 9,19 – 36, 38, 39, 48 – 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over in view of Drake et al. USPN 6,347,374 as applied in claim 1, in view of Sutton et al. USPN 5,920,719.

Regarding claim 2, Drake discloses all the claimed limitations as applied in claim 1. Drake doesn't explicitly disclose wherein said template comprises at least one constant element. Sutton discloses abstract as well as variable primitives allowing the user to extend data types used for information collection (9: 30 – 35). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Drake and Sutton because, using constant elements ensures more reusability of templates.

Regarding claim 3, the system of claim 2 wherein said at least one constant is included in verbatim in said output (Drake, 4: 5 – 10).

Regarding claim 4, Drake discloses all the claimed limitations as applied in claim 1. Drake doesn't explicitly disclose wherein said template comprises at least one variable element. Sutton discloses abstract as well as variable primitives allowing the user to extend data types used for information collection (9: 30 – 35). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Drake and Sutton because, using variable elements would make the templates more customizable.

Regarding claim 5, the system of claim 4 wherein said at least one variable element identifies a particular portion of the raw audit data to be included in said output (Drake, 4:3 – 25).

Regarding claim 6, wherein said at least one variable element identifies a particular portion of the raw audit data to be included in said output (Drake, 4:3 – 25).

Regarding claim 7, the system of claim 1 wherein said raw audit data comprises a record for each invocation of an operating system routine that is included within said raw audit data, and wherein each record includes at least one type of audit information relating to execution of an invoked operating system routine (Drake, Col.9: 20 – 35).

Regarding claim 8, the system of claim 7 wherein said at least one type of audit information includes at least one type selected from the group consisting of:

user identification, group identification, supplementary group identification, process identification, event identification, event count, event type, date, time, thread identification, system call, capabilities used, object, and result (Drake 5, 40 – 55).

Regarding claim 9, see reasoning in claim 4.

Regarding claim 19, the product version of the system in claim 3, see rationale as previously discussed above.

Regarding claim 20, the product version of the system in claim 4, see rationale as previously discussed above.

Regarding claim 21, the product version of the system in claim 7, see rationale as previously discussed above.

Regarding claim 22, the product version of the system in claim 8, see rationale as previously discussed above.

Regarding claim 23, the computer program product of claim 22 wherein said audit data comprises multiple ones of said record, further comprising code executable to sort at least a portion of the multiple records based on at least one of said types of audit information (Drake, 4: 20 – 24, see filter for sort).

Regarding claim 24, the product version of the system in claim 9, see rationale as previously discussed above.

Regarding claim 25, the product version of the system in claim 10, see rationale as previously discussed above.

Regarding claim 26, the method version of the system in claim 4, see rationale as previously discussed above.

Regarding claim 27, the method version of the product in claim 4, see rationale as previously discussed above.

Regarding claim 28, the method of claim 26 further comprising the step of creating, by a user, said audit transformation template (Drake, 16: 1 – 7).

Regarding claim 29, the method version of the system in claim 3, see rationale as previously discussed above.

Regarding claim 30, the method version of the system in claim 4, see rationale as previously discussed above.

Regarding claim 31, the method version of the system in claim 5, see rationale as previously discussed above.

Regarding claim 32, the method version of the system in claim 8, see rationale as previously discussed above.

Regarding claim 33, the method of claim 26 further comprising the step of: presenting said output to a user (Drake, 4:3 – 25).

Regarding claim 34, the method version of the system in claim 5, see rationale as previously discussed above.

Regarding claim 35,the method of claim 26 further comprising the step of inputting said output to an application for processing by said application (Drake, 4:3 – 25).

Regarding claim 36, the method of claim 26 further comprising the step of: sorting said raw audit data based at least in part on at least one type of audit information included therein (Drake, 17: 30 – 32, see filter and sort templates]).

Regarding claim 38, the software version of the system in claim 5, see rationale as previously discussed above.

Regarding claim 39, the library of claim 37 wherein said function executable to access raw audit data, said function executable to access a template, and said function executable to generate output are included within a common function (Drake, 21: 7 – 11).

Regarding claim 48, the method of claim 26 wherein said generating an output comprises:

generating an output presentation one see, displaying and printing statistical data (17: 55 – 58).

Regarding claim 49, the method of claim 28 wherein said presentation output presentation output comprises at least one selected from the group consisting of:

(for at least one see, displaying and printing statistical data 17: 55 – 58).

Regarding claim 50, which recites the method version of claim 42, see reasoning as previously discussed above.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Drake et al. USPN 6,347,374 as applied in claim 1, in view Maloney et al. USPN 6,253,337 Bl.

Regarding claim 12, Drake discloses all the claimed limitations as applied in claim 1. Drake doesn't expressly disclose wherein said template defines a format of a markup language. However, Maloney does disclose this feature in a similar configuration. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Drake with Maloney to implement the instant claimed invention because, use of the HTML format would made the system more distributed and internet compatible.

Response to Arguments

7. Applicant's arguments filed 04/06/2005 have been fully considered but they are not persuasive to overcome the previous rejection 01/06/2005.

Argument (1), Applicant argues on page 11 of Applicant's response (04/06/05) that in claims 1, 14, 37, and 54 that Drake doesn't teach " software code executable by at least one processor to receive said raw audit data and generate output comprising at least a portion of said raw audit data in a desired format defined by template".

Response (1), In 9: 45 – 60, Drake teaches a process, which includes the collector 26 and the parser 20, where the audit acquisitions (audit data) are unique to the audit source, and each audit source being unique (i.e., desired format), and further stating that there is a different collector for each operating system application on a given

format, Examiner interprets this to be the Equivalent function of Applicant's desired format defined by template, since different formats are able to be mapped to different formats, and Drake in 11, also discloses the use of Expert systems to convert data into different formats such as in the collection of statistical profiles, see 11:13 – 18.

Applicant argues on page 13 of Applicant's response (04/06/05) that claim 12, which is dependent on improperly rejected base claim (i.e. claim 1) under 35 U.S.C. § 102, is also improperly rejected under 35 U.S.C. § 103.

Examiner has addressed Applicants arguments with regards to 35 U.S.C. § 102, in claims 1, 14, 37 and 54, and hence arguments with regards to 35 U.S.C. § 103 have also been addressed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chuck Kendall whose telephone number is 571-272-3698. The examiner can normally be reached on 10:00 am - 6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Dam can be reached on 571-272-3695. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ck.

ANTONY NGUYEN-BA
PRIMARY EXAMINER